了解Umbrella中的公钥固定和证书固定

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[概述](#)

[兼容Umbrella SWG](#)

[其他证书固定应用](#)

简介

本文档介绍Cisco Umbrella中的证书固定和公共密钥固定。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco Umbrella。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

证书固定是一种互联网安全机制，允许应用使用错误颁发的或以其他方式欺诈的数字证书来抵制对HTTPS服务器的模拟。它通过将服务器与一组已定义的公钥关联来达到此目的，这些公钥可能是唯一可信任的，可用于与该服务器的连接。证书固定有两种技术：

- 公钥固定(PKP RFC7469)是一种现在过时的机制，用于在Web浏览器中触发证书固定。固定证书将使用HTTP标头发送到浏览器。
- 静态证书固定是指对应用进行硬编码，以便期望特定证书或证书颁发机构。某些桌面/移动应用使用静态证书固定机制来提高安全性。

当这些Web应用程序由Umbrella代理时，Umbrella提供的公钥不匹配，从而导致应用程序关闭HTTPS连接。证书固定通常仅适用于桌面/移动应用，因为现代Web浏览器已删除PKP支持。

兼容Umbrella SWG

Umbrella在某些情况下会绕过来自SSL解密的已知URL，以解决证书固定问题。表1包括所有Umbrella客户已全局绕过的应用程序。表1还包括在当时或写入时已知使用证书定位的其他应用。如果您使用的是这些应用程序中的任意一个，则可以考虑使用后面介绍的方法（出于给出的原因）从HTTPS检查中绕过应用程序。表2提供了表1中涵盖的应用程序服务的更多详细信息。

其他证书固定应用

使用Umbrella的[Selective Decryption](#)（选择性解密）功能，可以按客户（按策略）绕过应用，以解决证书固定问题。这些例外可以根据域、应用名称或类别轻松实施；Umbrella SWG在我们的应用数据库中包含大型应用库。

在大多数情况下，是否绕过应用由IT管理员决定。添加解密例外是一种安全权衡，因为它会阻止对Web内容进行安全/文件检查。这是一个独立的决策，取决于应用类型和业务需求。例如，如果证书固定问题仅影响移动/桌面应用，管理员可以选择添加例外来使移动应用工作，或者更愿意让用户使用该应用的Web版本。

这是一个应用表，这些应用对于Umbrella客户而言是全局绕过的，且在编写时不需要或已知任何操作来使用证书固定，并且在默认情况下不被Umbrella绕过。如果您使用的是默认情况下未绕过的应用，则可以考虑使用上述方法（出于给出的原因）从HTTPS检测中绕开应用。

表1 - 可使用证书固定的应用

应用程序名称	思科Umbrella覆盖
Adobe服务	Umbrella客户在全球范围内绕过
Airbnb	由应用控制支持
亚马逊Alexa	由应用控制支持
Amazon Drive	由应用控制支持
亚马逊Kindle	由应用控制支持
Amazon工作空间	由应用控制支持
振幅	Umbrella客户在全球范围内绕过

应用动态	Umbrella客户在全球范围内绕过
Apple iMessage	由应用控制支持
Apple邮件	由应用控制支持
Apple服务(有关更多详细信息，请参阅表2)	Umbrella客户在全球范围内绕过
思科服务(详情请参阅表2)	Umbrella客户在全球范围内绕过
Citrix工作空间	由应用控制支持
脆裂剂	Umbrella客户在全球范围内绕过
CrowdStrike猎鹰	由应用控制支持
Diligent.com	由应用控制支持
不和谐聊天	Umbrella客户在全球范围内绕过
DocuSign协议云	由应用控制支持
DropBox	由应用控制支持
Druva云备份	由应用控制支持
Egnyte连接	由应用控制支持
Evernote	由应用控制支持
Facebook Messenger	由应用控制支持
脸书	由应用控制支持
文件电邮	由应用控制支持

四方	由应用控制支持
Giphy	Umbrella客户在全球范围内绕过
Github	由应用控制支持
Google Drive	由应用控制支持
Google Play商店	由应用控制支持
Google服务(有关更多详细信息，请参阅表2)	Umbrella客户在全球范围内绕过
谷歌工作空间	由应用控制支持
转到会议	由应用控制支持
炒作机	由应用控制支持
Instag	由应用控制支持
LogMein Pro	由应用控制支持
Microsoft Defender for Endpoint	由应用控制支持
Microsoft Intune	由应用控制支持
Microsoft服务(有关更多详细信息，请参阅表2)	Umbrella客户在全球范围内绕过
Microsoft Xbox Live	由应用控制支持
Netflix	由应用控制支持
OpenDrive	由应用控制支持
PayPal	由应用控制支持

PingOne身份	由应用控制支持
机架空间/云驱动器服务	Umbrella客户在全球范围内绕过
Salesforce CRM	由应用控制支持
网段	Umbrella客户在全球范围内绕过
信号平台	由应用控制支持
Skype for Business	由应用控制支持
Snapchat	由应用控制支持
Soundcloud	由应用控制支持
SpiderOak	由应用控制支持
Spotify	由应用控制支持
团队查看器	由应用控制支持
抖音	由应用控制支持
托多伊斯特	由应用控制支持
推特	由应用控制支持
维密欧	由应用控制支持
工作日HCM	由应用控制支持
缩放会议	Umbrella客户在全球范围内绕过

表2 -详细信息全局绕过的服务，如表1所示

Apple服务	<ul style="list-style-type: none"> • Apple强制网络门户检查 • Apple iTunes和应用商店 • 其他苹果平台服务
Cisco 服务	<ul style="list-style-type: none"> • Cisco Umbrella和OpenDNS服务 • Cisco Webex和Webex团队 • 思科云邮件安全WebUI • AMP终端服务 • Duo Security 2FA
Google服务	<ul style="list-style-type: none"> • Google Hangouts • Web上的Google消息 • 其他Google平台服务
Microsoft服务	<ul style="list-style-type: none"> • Microsoft网络连接状态指示灯 • Windows更新 • Windows翻译服务 • 其他Microsoft/Windows平台服务

有关其他帮助，请参阅排除非浏览器应用程序故障或与[Umbrella支持联系](#)。在工程团队审核后，可以考虑将应用添加到我们的全局旁路列表。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。